10/577158

SUBSTITUTE SPECIFICATION Rec'd PCT/PTO 26 APR 2006

METHOD FOR MANAGING THE SECURITY OF APPLICATIONS WITH A SECURITY MODULE

Field of the invention

[0001] The present invention concerns the domain of mobile networks also called cellular networks. More particularly, it concerns the management of the security of the applications that function with a security module associated to a mobile equipment of mobile telephony.

Technical background

[0002] The security module of a mobile or portable telephone is known under the denomination "SIM card" (Subscriber Identity Module) that constitutes the central security element of these telephones. The telephone operator introduces, during manufacturing and/or during the personalization stage, a number called IMSI (International Mobile Subscriber Identification) that serves to identify in a secure and unique way each subscriber desiring to connect to a mobile network. Each mobile telephone, called mobile equipment hereinafter, is physically identified by a number stored in a non-volatile memory of the mobile equipment. This number, called IMEI, (International Mobile Equipment Identifier) contains an identification of the type of mobile equipment and a serial number serving to identify in a unique way a given mobile equipment on a network of the GSM type (Global System for Mobile Communications), GPRS (General Packet Radio System) or UMTS (Universal Mobile Telecommunications System). Furthermore, mobile equipment is characterized by a software version SVN (Software Version Number) indicating the updating state of the base software installed on the mobile equipment. The combination of the identification of the type and of the serial number of the mobile equipment with the software version (SVN) gives a new identification, called IMEISV (International Mobile Equipment Identifier and Software Version Number). The same identification concept also applies to the WLAN (Wireless LAN) or to bidirectional cable TV. The physical identifier can be a MAC address (Media Access Control) that corresponds to the unique address that identifies the configuration of the material of a user on a network IP (Internet Protocol) and the software version can be transmitted by upper layer protocols based on IP.

[0003] The ETSI regulations ("European Telecommunications Standards Institute"), define a mobile station (MS, mobile station) composed of an item of mobile equipment (ME, mobile equipment) and a subscription module (SIM, subscriber identity module). This subscriber module is usually removable, that is to say that it can be either withdrawn or transferred from one item of mobile equipment to another.

[0004] During the activation of a mobile equipment, more particularly during its connection to the network of an operator, data comprising the identification data is exchanged between the mobile equipment and the management center of the operator that authorizes or prohibits its use.

[0005] The document EP0757502 describes a method of locking a user identification module when the physical identifier of the mobile equipment IMEI is on a black list. When the mobile equipment connects to the mobile network, it transmits the identifier IMEI to a management center. The latter makes a comparison to verify the identifier received with the contents of a database where the operator registers the identifiers of stolen or defective mobile equipments. If an identifier received is present in this database, the management center transmits a message containing a locking command to the mobile equipment in question. This command, after verification of its authenticity, is transmitted to the identification module that carries out a locking procedure preventing any further connection of the mobile equipment to the network.

[0006] The document US5864757 describes an activation method of a mobile handset with a subscriber module based on the use of a key pertaining to the handset producing a code corresponding to an identifier of the subscriber module. The handset includes a single tamper-proof key. At the time of its activation, the operator's management center transmits a message to the handset serving to calculate a key specific to the operator by using the unique key of the handset. This new key is used in combination with an identifier of the network or of the subscriber module to generate a control word that is confronted with a code stored in the subscriber module. If the control word agrees with the subscriber module code, the handset is activated.

[0007] The methods described in these two documents exclusively concern aspects requiring the physical identification of the mobile equipment based, for example, on the identifier IMEI. When these methods are implemented, their effects concentrate only on the locking / unlocking of the subscriber module and/or of the mobile equipment in order to prevent any connection of the mobile equipment to the network.

[0008] Presently, mobile equipment offers to the user, in addition to its usual function of establishing telephone conversations by means of an access to a mobile network, the use of numerous other supplementary value added services such as the consultation of various information, remote banking transactions, electronic commerce, access to multimedia contents, etc. These improved services require an increasingly higher level of security in order to protect users against possible frauds caused by third parties seeking to exploit security failures that may appear on the mobile equipments.

[0009] Therefore, verification on at least two levels becomes necessary: on one hand at the level of the mobile equipment itself and on the other hand at the level of software applications that allow the functioning of the different services proposed by the operator or by third parties. The aim is to guarantee that the subscriber module operates only with mobile equipment of the type and software version duly authorized or homologated by the operator and/or by the application suppliers. Functioning of the subscriber module is understood to mean the capacity to allow the use of services requested by a user by carrying out a certain number of software applications previously installed in a memory of the mobile equipment and which use the subscriber module as protection mean.

[0010] These applications carried out in the mobile equipment use resources available in the subscriber module. Resources are understood to mean different functions and data necessary for the correct functioning of an application. Certain resources can be common to several applications, in particular the functions related to security. The subscriber module can thus block or alter the functioning of certain applications for which the security conditions established by the operator and/or application supplier are not respected in the mobile equipment in question or the rights of the user of the mobile equipment are insufficient.

[0011] The aforementioned documents do not cover the software aspects related to a group of mobile equipments such as, for example, information related to software applications installed, a software version number or even a reference to a type or to a model of mobile equipment, etc. Therefore, it concerns the use of a targeted management method of resources of the subscriber module in order to selectively activate / deactivate the applications or application functions using these resources. However, it is not desirable for these operations to prevent the mobile equipment from accessing the network by completely locking the subscriber module.

Summary of the invention

[0012] The aim of this invention is to propose a management method for the security of the set mobile equipment, subscriber module and applications in order to limit risks related to the fact that a subscriber module could be fraudulently used by applications carried out on a mobile equipment of a type and/or of a software version that fails to fulfill certain predetermined security criteria.

[0013] Another aim is to protect the user of the mobile equipment as well as the application suppliers against abuses resulting from the cloning of the mobile equipment and/or of the subscriber module.

[0014] These aims are achieved by means of a method for managing the security of applications with a security module functioning in an equipment connected to a network, said network being administrated by a control server of an operator, said applications using the resources (data or functions) stored in a security module connected locally to said equipment, comprising the following preliminary steps:

- reception of data comprising at least the type and software version of the equipment and the identity of the security module, via the network, by the control server,

- analysis and verification by the control server of said data,

- generation of a cryptogram from the result of the verification on said data, and transmission of said cryptogram, via the network and the equipment, to the security module,

said method is characterized in that the security module analyses the cryptogram received and activates, respectively deactivates the resources (data or functions) used by at least one application installed in the equipment, said cryptogram comprising instructions conditioning the functioning of the application according to criteria predetermined by the supplier of said application and/or the operator and/or the user of the equipment.

[0015] The resources of the subscriber module are blocked in a targeted way, in order to block or reduce the function of certain applications. The applications of the equipment are not directly blocked: one act indirectly on the applications, that is to say that the blocking effect will be noticed only when the equipment attempts to carry out these applications.

[0016] This method applies preferably to the mobile network. Consequently, the equipment is a mobile equipment, such as for example an equipment of mobile telephony or a portable telephone. The security module is a subscriber module inserted into the mobile telephone that is of the SIM card type (subscriber identity module). This assembly connects to a mobile network of the type GSM (Global System for Mobile communications), GPRS (General Packet Radio System), UMTS (Universal Mobile Telecommunications System) or the like, managed by a control server of an operator. Software applications are installed on the mobile equipment and configured in order to use the resources (data or functions) present in the subscriber module. They can thus be used in their entirety only if the security conditions are satisfied according to criteria predetermined by the operator and/or the application supplier. This verification of the criteria is in charge of the control server. The application, following the instructions sent by the control server, is finally in charge of the security module that can free or block the access to the resources necessary for the correct functioning of an application installed in the mobile equipment.

[0017] The data of these resources can comprise data such as account numbers, programs (in the form of code that can be installed in the mobile equipment), encryption/decryption keys, access rights to contents, etc.

[0018] The functions of these resources can include cryptographic algorithms, verification processes, digital signature generation processes, encryption processes, authentication process, data validation processes, access control processes, data security processes, payment processes etc.

[0019] The control server plays an essential role in managing the trust or security elements related to the set mobile equipment / subscriber module. It interprets the data that is transmitted by the mobile equipment in order to control or limit the use of applications, functions or resources available by means of the subscriber module.

[0020] The server receiving the identity information from a mobile equipment and its subscriber module and comprising IMEISV and IMSI decides, according to certain criteria, if a new instruction must be sent to the subscriber module to redefine a new protection profile that defines the resources of the subscriber module that can be used by applications executed in the mobile equipment. The criteria can refer, for example, to the updating of the software version installed on the mobile equipment, to the downloading of new applications on the mobile equipment, to the updating period of the protection profile, to a number of connections to the network, to the technology used for access to the network and to the identity of the access network used. These criteria are also related to different risks associated with the material or software used that the operator and/or the application supplier and/or the user of the mobile equipment wishes to take in account.

[0021] The method according to the invention is generally carried out during each connection of the mobile equipment to the network or after each update of the software version of the mobile equipment or of that of the subscriber module or even of that of resources on the subscriber module. It can also be carried out during each activation or deactivation of an application on the mobile equipment.

[0022] According to one embodiment, it can be carried out periodically at a rate given by the control server or after each initialization of an application on the mobile equipment. According to another embodiment, the subscriber module will not receive a new message from the control center as long as the identifier IMEISV of the mobile equipment remains unchanged.

[0023] During the re-initialization of the subscriber module, it is preferable to block a certain number of resources until the arrival of the cryptogram. Therefore, if the mobile equipment wants to intercept the cryptogram and not transmit it to the subscriber module, all or part of the resources (data or functions) of the subscriber module will be unavailable for applications carried out in the mobile equipment. According to the type of realization, it is possible that certain resources of the subscriber module used by low security level applications are implemented by default before the arrival of the cryptogram. This is also the case for resources necessary to obtain access to the network, without this the sending of the cryptogram would not be possible by this same network.

[0024] When the subscriber module verifies the validity of the cryptogram, it also indirectly identifies the mobile equipment and ensures that the data is effectively coming from the control server. In other words, by means of this cryptogram, the control server implicitly ensures the subscriber module that the type and the software version of the mobile equipment have been taken into account before transmitting instructions to the subscriber module. The latter are, in fact, loaded, if necessary, to give or refuse complete or partial authorization for the use of certain applications of the mobile equipment.

[0025] The mobile equipment plays the role of a relay in this verification step by establishing an almost direct dialogue between the subscriber module and the control server. Therefore the security of the exchanged messages is ensured from end to end between the control server and the subscriber module via the execution environment of the applications implemented on the mobile equipment. This cannot thus "cheat" or transform the data in relation to the subscriber module.

[0026] This invention also concerns a security module comprising the resources destined to be accessed locally by at least one application installed in an equipment connected to a network, said equipment comprising reading and data transmission means comprising at least the type and software version of the equipment and the identifier of the security module, said module being characterized in that it includes means for reception, analysis and execution of instructions contained in a cryptogram, said instructions conditioning the functioning of the

application according to criteria predetermined by the supplier of said application and/or the operator and/or the user of the equipment.

[0027] This security module is used for example as a subscriber module or SIM card connected to a mobile equipment.

Brief description of the drawings

[0028] The invention will be better understood thanks to the following detailed description that refers to the enclosed figures given as a non-limitative example, namely:

- Figure 1 illustrates a block diagram showing the different parts of the mobile equipment and of the server that contribute during the exchanges of identification data and of the cryptogram.

- Figure 2 represents a block diagram of the mobile equipment / subscriber module assembly with interactions between the different parts during the functioning of an application.

Detailed description

[0029] Figure 1 shows the mobile equipment (CB) and subscriber module (SIM) assembly that transmits, via a mobile network (NET), identification data (ID) that is verified by the control server (CSE). The latter sends back a cryptogram (J) towards the subscriber module via the mobile equipment (CB). The mobile equipment (CB) includes one or more software applications (APP) working in an execution environment (AEE). These applications are provided either by an application supplier (FA) associated with the control server (CSE) of the operator, or they are originally programmed by the manufacturer of the mobile equipment.

[0030] The subscriber module includes resources (RES) used by software applications (APP).

[0031] Figure 2 shows that the functioning of the applications (APP) of the mobile equipment (CB) depends directly on the resources (RES) available in the

subscriber module. In the absence of adequate resources, the application can either not be started or it functions in a very limited way with default parameters that can generate error messages inviting the user to complete the necessary corrective actions such as, for example, the changing of mobile equipment (CB) or of subscriber module (SIM).

[0032] The mobile equipment (CB) is identified, for example, during each request for connection to the network, to the control server (CSE) via the mobile network (NET) by transmitting preferably data specific to mobile equipment: IMEISV (International Mobile Equipment Identity and Software Version Number) and a subscriber module code: IMSI (International Mobile Subscriber Identity). The first number IMEISV is a set of 16 digits containing in particular an homologation code from the mobile equipment manufacturer, a serial number that physically identifies the mobile equipment in a unique way and the software version installed on the mobile equipment in question. The number second IMSI is a set of 15 digits and includes a code attributed by the operator, with which a user has subscribed to a subscription, allowing the identification of a subscriber in a unique way. For mobile equipment produced according to previous standards established by ETSI (European Telecommunications Standards Institute), the combination of the number IMEI composed of a set of 15 digits and of the number SVN composed of a set of 2 digits also provides the data necessary for the implementation of the method.

[0033] During the identification of mobile equipment, the control server (CSE) analyses and verifies the data (ID) transmitted and compares it with the contents of a black list (data to reject) or with a white list (accepted data). A database allows the refinement, if necessary, of the identification of a subscriber and the determination of his details such as authorized services, subscription payments and/or services executed or not, subscription period, security profile associated to the mobile equipment used, applications installed on the mobile equipment, resources available on the security module, preferences of the mobile equipment user, etc. The results of this verification are then used in order to determine a cryptogram, called a token (J), that the control server (CSE) transmits to the mobile equipment (CB). It should be noted that the control server (CSE) can be distinct from the mobile operator and the

request coming from the mobile equipment will be forwarded towards this control authority.

[0034] The application execution environment (AEE) of the mobile equipment (CB) transmits the token (J), as it is, without altering it, to the subscriber module, the mobile equipment (CB) playing only a role of relay.

[0035] If the token (J) is valid, the subscriber module can free, respectively block certain resources (RES). The application(s) (APP) can thus be executed according to the criteria imposed by the control server (CSE). In fact, the token (J) includes or is accompanied by particular instructions intended for the subscriber module that can condition the functioning of any of the applications (APP) of the mobile equipment (CB). For example the execution of financial transactions can be limited when the subscriber is connected to another network to which he is subscribed, for example, in a country different to his country of residence (roaming) due to certain security criteria or preferences of the subscriber or preferences of the financial service supplier or due to legal constraints in force in the country in question. In another case, when a subscriber module is inserted into a mobile equipment (CB) not recognized or not homologated by the operator, the token (J) returned by the control server (CSE) can block the resources (RES) of the subscriber module and in this way prevent or alter the execution of an application(s) (APP).

[0036] In the case of a possible cloning of the mobile equipment (CB) and/or of the subscriber module (SIM), the results of the verification with the database include instructions depending on the risk that the operator accepts to take with cloned mobile telephones. For example, the token (J) generated as a result can either block all the resources (RES) of the subscriber module, or limit their use during a period of time and/or create a warning message for the subscriber via the execution environment of the applications (AEE).

[0037] The token (J) can, for example, be associated to a signature generated with the aid of a private key RSA, (Rivest, Shamir, Adelman) KRSA_Prri from a data set containing, for example, IMSI, IMEISV, the resources references of the subscriber module, a counter. This key would be known only by the control server while its public part KRSA_Pub would be known by the subscriber module. The advantage of

the use of asymmetric keys resides in the fact that the key serving to create signatures is not found outside the control server (CSE).

[0038] Of course, other asymmetric key algorithms such as, for example, DSA (Digital Signature Algorithm), and ECC (Elliptic Curve Cryptography) can be used as an alternative to RSA.

[0039] The use of symmetrical key algorithms may be preferred for reasons concerning simplicity, speed of verifications or lower costs for manufacturing and implementation. In this case, the key would be known by the server (CSE) and by the subscriber module, for example, an algorithm IDEA (International Data Encryption Algorithm) could be used to sign the assembly (IMSI, IMEISV, resources reference of the subscriber module, counter). As an alternative to the IDEA algorithm, algorithms such as, for example, TDES (Triple Data Encryption Standard) and AES (Advanced Encryption Standard) can also be used.

[0040] In these two asymmetrical and symmetrical key embodiments, the subscriber module verifies the correspondence of the different fields appearing in the token (J), in particular it controls the counter (CPT) by comparing it with a corresponding counter stored in the card which is regularly updated. This counter allows avoiding the double use of the same token (J) intended for the subscriber module in order to prevent a replay attack.

[0041] An embodiment to the counter is the use of a random variable (random number) generated by the subscriber module. This random variable is transmitted with the data sent to the control server. The latter sends back this random variable in the response cryptogram and the subscriber module can verify that it concerns a new message. More generally, in order to avoid all risk of the use of an old cryptogram, the latter includes a variable predictable for the subscriber module, either a counter or a random variable.

[0042] The subscriber module also considers the resource reference (RES) that will authorize or prohibit the use by applications carried out in the mobile equipment (CB).

[0043] The subscriber module does not know as such the application references (APP) installed in the mobile equipment (CB). In fact, certain more global applications have a relatively open interface that allows them to be used for any external secondary applications. For example, it is possible to graft particular applications onto a general payment application according to the mode of payment used. The subscriber module can only be based on the references of its own resources (RES) (data or functions). By accepting the risks related to a mobile equipment, the operator makes a choice by knowing which resources (RES) of the subscriber module are used by which application(s) (APP) executed in the mobile equipment (CB).

[0044] In another embodiment, the signature made with the aid of a key of the RSA or IDEA type can be replaced by a block generated with a shared key HMAC (Keyed-Hashing for Message Authentication) from the set (IMSI, IMEISV, resource references of the subscriber module, counter). HMAC is a mechanism for message authentication through the use of cryptographic hashing functions such as MD5 (Message Digest) or SHA-1 (Secure Hash Algorithm), in combination with a shared key, namely the same key is located in the control server (CSE) and in the subscriber module.

[0045] This key, that is present at the same time in the control server (CSE) and in the subscriber module, can be loaded during the personalization of the subscriber module or during the installation of certain resources in the subscriber module. According to the options, a different key can be associated to each resource or resource group of the subscriber module, or the key can be global for the resource assembly and unique for a given subscriber module.

[0046] For more security, when the subscriber module has received a token (J), it can retransmit to the control server (CSE), via the mobile equipment (CB) and the mobile network (NET), a confirmation message (CF) confirming the correct reception and adequate processing of the token (J) by the subscriber module. The confirmation (CF) includes at least one success or error code for the operation as well as a counter, similar to that of the token (J), serving to protect against replay attacks. This message also allows the control server (CSE) to maintain updated the counter associated to the subscriber module.

[0047] In an embodiment of the invention, the mobile equipment can be replaced by non-mobile equipment such as a Pay-TV decoder or a computer. The control server receives from the security module, the equivalent of the subscriber module, the identifier of the equipment connected to the network and the identifier of the security module. In response, the server carries out the verifications as described previously and sends back a cryptogram to the security module. This response will free or block resources in the security module.